1 Общие замечания

Данный текст представляет из себя краткий конспект лекций по курсу «Математическая логика», рассказанных студентам ИТМО (группы 2538 и 2539) в 2011-2012 учебном году.

2 Язык исчисления высказываний

Определение 2.1. Языком исчисления высказываний мы назовем язык L, порождаемый следующей грамматикой со стартовым нетерминалом `<выражение>`:

<выражение> ::= <импликация>
<импликация> ::= <дизъюнкция> | <дизъюнкция> $\to$ <импликация>
<дизъюнкция> ::= <конъюнкция> | <дизъюнкция> $\vee$ <конъюнкция>
<конъюнкция> ::= <терм> | <конъюнкция>&<терм>
<терм> ::= <пропозициональная переменная> | (<выражение>) | $\neg$<терм>

Нетерминал <пропозициональная переменная> формально определять не будем, хотя это можно также сделать ценой небольшого технического усложнения. Договоримся, что такие переменные — это большие буквы латинского алфавита, возможно, имеющие нижний индекс.

Так построенная грамматика предписывает определенный способ расстановки опущенных скобок, при этом скобки у конъюнкции и дизъюнкции расставляются слева направо, а у импликации — справа налево (это соответствует традиционному чтению), так что выражение $A \to B\&C\&D \to E$ следует понимать как $A \to (((B\&C)\&D) \to E)$. Все выражения, которые отличаются только наличием дополнительных незначащих скобок (не изменяющих порядок операций), мы будем считать одинаковыми.

В случаях, когда это будет существенно, мы будем дополнительно ограничивать свободу расстановки скобок, требуя указывать скобки для всех двуместных операций:

<выражение> ::= <импликация>
<импликация> ::= <дизъюнкция> | (<дизъюнкция> $\to$ <импликация>)
<дизъюнкция> ::= <конъюнкция> | (<дизъюнкция> $\vee$ <конъюнкция>)
<конъюнкция> ::= <терм> | (<конъюнкция>&<терм>)
<терм> ::= <пропозициональная переменная> | <выражение> | $\neg$<терм>

Обратите внимание, в такой грамматике каждая двуместная операция указывается вместе со скобками, и при этом «незначащие» скобки запрещены. Поэтому здесь есть только один способ записать данное выражение.

Все формулы, порождаемые данными грамматиками, мы будем называть *высказываниями* (также формулами или выражениями исчисления высказываний). Высказывания, подробности которых нас не интересуют, мы будем обозначать начальными буквами греческого алфавита (α, β, γ и т.п.).

Теперь попробуем научиться вычислять значение высказываний. Зададим некоторое множество истинностных значений V и функции оценки $f_\&, f_\vee, f_\to : V \times V \to V$, и $f_\neg : V \to V$, по функции на каждую из связок и на отрицание. Также зададим *оценку* переменных, функцию, сопоставляющую множеству переменных P некоторого высказывания α — функцию $f_P : P \to V$.

Определение 2.2. Если дано некоторое высказывание α, в котором используются пропозициональные переменные $v_1 \dots v_n$, то *оценку* данного высказывания $|\alpha|$ мы определим следующим рекурсивным образом.

Возьмем дерево разбора высказывания, и возьмем его корень. В зависимости от правила, по которому получен корень, результатом оценки мы назовем:

- пропозициональная переменная v_i: $f_P(v_i)$
- конъюнкция выражений α и β: $f_\&(|\alpha|, |\beta|)$
- дизъюнкция выражений α и β: $f_\vee(|\alpha|, |\beta|)$
- импликация выражений α и β: $f_\rightarrow(|\alpha|, |\beta|)$
- отрицание выражения α: $f_\neg(|\alpha|)$
- во всех остальных случаях оценка выражения равна оценке потомка в дереве.

Теорема 2.1. Данное определение позволяет оценить любое выражение.

Доказательство. Утверждение очевидно, но для демонстрации техники стоит доказать.

Докажем индукцией по длине формулы, n; это традиционный способ доказательств различных фактов про выражения. Данное доказательство подходит для первого варианта грамматики.

База: $n = 1$. Анализ грамматики показывает, что такая строка может состоять только из имени пропозициональной переменной. Очевидно, что указанный способ оценки позволяет такую строку оценить всегда.

Переход: пусть $n \geq 1$ и для n все доказано. Рассмотрим строку длины $n + 1$. В дереве разбора данной строки есть некоторый корень, рассмотрим его. Он может быть:

- термом — при этом это не пропозициональная переменная, так как длина строки больше 1. Значит, это либо выражение в скобках — тогда все доказано по предположению индукции, поскольку длина выражения в скобках — $n - 1$, либо отрицание. Тогда применение функции $f_\neg$ к оценке строки длины n даст оценку выражения.
- импликацией, конъюнкцией или дизъюнкцией, при этом примененный вариант правила добавляет новые терминальные символы в строку. Значит, здесь дерево разбора разделит строку на две, причем длины строго меньшей, чем n. В этом случае очевидно, что значение выражения будет вычислено.
- выражением, импликацией, конъюнкцией или дизъюнкцией, при этом примененный вариант правила не добавляет новых терминальных символов. В этом случае, спустившись (возможно, несколько раз) вниз по дереву мы дойдем либо до терма, либо до вариантов правил для импликации, конъюнкции или дизъюнкции, добавляющих терминальные символы, и окажемся в условиях предыдущих пунктов.

□

Зафиксируем множество истинностных значений V. Для дальнейшего изложения в качестве множества V нам будет достаточно взять {И,Л} (*И* обозначает истину, *Л* обозначет ложь).

Также зафиксируем функции оценки для связок и отрицания (они вполне традиционны, для примера приведем таблицу истинности для импликации).

α	β	$\alpha \to \beta$
Л	Л	И
Л	И	И
И	Л	Л
И	И	И

Отметим, что хоть данные определения в целом повторяют традиционные, они построены таким образом, чтобы допускать различные обобщения в случае необходимости. Мы будем время от времени этой возможностью пользоваться.

Также заметим, что единственный произвол в оценке выражения связан с выбором оценки для пропозициональных переменных f_P.

Определение 2.3. Назовем высказывание `общезначимым`, если его оценка истинна при любой оценке входящих в него пропозициональных переменных. На языке исследователя будем также записывать это так: $\models \alpha$.

3 Формальная система и исчисление высказываний

Определение 3.1. *Формальная система* – это упорядоченная тройка $\langle L, A, R \rangle$, где L – некоторый язык, $A \subset L$ – множество *аксиом*, а $R \subset (L^2 \cup L^3 \cup L^4 \cup \ldots)$ – множество *правил вывода.*

Поясним определение. Множество L содержит все выражения, которые мы считаем допустимыми (корректно сформированными). Множество аксиом A — это некоторые корректно сформированные выражения, которые мы принимаем без доказательства. Правила вывода (элементы R) – это некоторые упорядоченные n-ки ($n \geq 2$) выражений, где первые $n-1$ выражений называются *посылками* рассматриваемого правила, а последнее выражение — *заключением* правила.

Определение 3.2. *Доказательство* в формальной системе $\langle L, A, R \rangle$ — это некоторая конечная последовательность выражений α_1, α_2 $\ldots \alpha_n$ из языка L, такая, что каждое из утверждений $\alpha_i (1 \leq i \leq n)$ либо является аксиомой (т.е. $\alpha_i \in A$), либо получается из других утверждений α_{P_1}, α_{P_2} $\ldots \alpha_{P_k}$ $(P_1 \ldots P_k < i)$ с использованием какого-нибудь правила вывода: $(\alpha_{P_1}, \alpha_{P_2} \ldots \alpha_{P_k}, \alpha_i) \in R)$.

Определение 3.3. Высказывание α называется доказуемым, если существует доказательство α_1, $\alpha_2 \ldots \alpha_k$, и в нем α_k совпадает с α.

В качестве сокращения записи в языке исследователя мы будем писать $\vdash \alpha$, чтобы сказать, что α доказуемо.

Расширим грамматику из предыдущего раздела:

<выражение> ::= <конъюнкция> | ψ | ϕ | π
<конъюнкция> ::= <дизъюнкция> | <дизъюнкция> $\to$ <конъюнкция>
<дизъюнкция> ::= <конъюнкция> | <дизъюнкция> $\vee$ <конъюнкция>
<конъюнкция> ::= <терм> | <конъюнкция>&<терм>
<терм> ::= <пропозициональная переменная> | (<выражение>)

Данная грамматика допускает дополнительные выражения, в которые входят буквы греческого алфавита ψ, ϕ и π. Все такие выражения мы назовем *схемами выражений*:

потому что если мы вместо *всех* данных букв подставим корректные выражения, соответствующие исходной грамматике языка, мы получим корректное выражение, принадлежащее исходному языку. При этом замена должна происходить согласованно — то есть, одинаковые буквы заменяются на одинаковые выражения. Все выражения, которые получены из схемы путем подстановки выражений вместо букв ψ, ϕ и π, мы назовем выражениями, *порожденными* схемой.

Определение 3.4. Исчисление высказываний — формальная система, использующая в качестве языка язык исчисления высказываний из предыдущего раздела, в качестве аксиом — аксиомы, порожденные следующими схемами выражений (в соответствии с расширенной грамматикой, указанной выше):

(1) $(\phi) \rightarrow ((\psi) \rightarrow (\phi))$
(2) $((\phi) \rightarrow (\psi)) \rightarrow ((\phi) \rightarrow (\psi) \rightarrow (\pi)) \rightarrow ((\phi) \rightarrow (\pi))$
(3) $(\phi) \rightarrow (\psi) \rightarrow (\phi)\&(\psi)$
(4) $(\phi)\&(\psi) \rightarrow (\phi)$
(5) $(\phi)\&(\psi) \rightarrow (\psi)$
(6) $(\phi) \rightarrow (\phi) \vee (\psi)$
(7) $(\psi) \rightarrow (\phi) \vee (\psi)$
(8) $((\phi) \rightarrow (\pi)) \rightarrow ((\psi) \rightarrow (\pi)) \rightarrow ((\phi) \vee (\psi) \rightarrow (\pi))$
(9) $((\phi) \rightarrow (\psi)) \rightarrow ((\phi) \rightarrow \neg(\psi)) \rightarrow \neg(\phi)$
(10) $\neg\neg(\phi) \rightarrow (\phi)$

в качестве правил вывода — все правила, порожденные согласованной заменой греческих букв в тройке схем выражений $\langle \phi, (\phi) \rightarrow (\psi), \psi \rangle$.

Традиционно правила вывода записывают так:

$$\frac{\phi \quad (\phi) \rightarrow (\psi)}{\psi}$$

4 Теорема о дедукции

Соглашение об обозначениях. Будем обозначать буквами Γ, Δ, Σ списки формул (возможно, пустые).

Определение 4.1. Вывод из допущений. Пусть Γ – некоторый список высказываний, а α — некоторе высказывание в исчислении высказываний $\langle L, A, R\rangle$. Тогда мы будем говорить, что формула α выводится из Γ (и записывать это как $\Gamma \vdash \alpha$), если существует доказательство формулы в исчислении $\langle L, A_1, R\rangle$, где A_1 – это A с добавленными формулами из Γ. Элементы Γ мы будем называть допущениями, предположениями или гипотезами.

Важно отметить, что поскольку речь идет о дополнительных предположениях, то тут говорят уже не о доказательстве, а о выводе. И, соответственно, о выводимости вместо доказуемости.

Очевидно, что если Γ — пустой список, то тогда $\Gamma \vdash \alpha$ соответствует $\vdash \alpha$.

По стилю записи такая конструкция напоминает импликацию, сейчас мы покажем, что между этой конструкцией и импликацией действительно есть связь.

Теорема 4.1. Пусть справедливо $\Gamma \vdash \alpha \to \beta$. Тогда также справедливо, что $\Gamma, \alpha \vdash \beta$.

Доказательство. Для получения требуемого вывода возьмем вывод формулы $\alpha \to \beta$, то есть некоторую последовательность формул $\delta_1 \dots \delta_{m-1}; \alpha \to \beta$. Добавим к выводу 2 формулы:

$(m+1)$	α	«Свежедобавленная» аксиома
$(m+2)$	β	М.Р. m, $m+1$

□

Теперь докажем обратное.

Лемма 4.2. $\vdash \alpha \to \alpha$

Доказательство. :

(1)	$\alpha \to (\alpha \to \alpha)$	Сх. акс. 1
(2)	$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	Сх. акс. 2
(3)	$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to (\alpha \to \alpha)$	М.Р. 1,2
(4)	$(\alpha \to ((\alpha \to \alpha) \to \alpha))$	Сх. акс. 1
(5)	$\alpha \to \alpha$	М.Р. 4,3

□

Теорема 4.3. Теорема о дедукции Пусть справедливо $\Gamma, \alpha \vdash \beta$. Тогда также справедливо $\Gamma \vdash \alpha \to \beta$.

Доказательство. Нам необходимо построить вывод утверждения $\Gamma \vdash \alpha \to \beta$ по имеющемуся выводу $\delta_1 \dots \delta_{m-1}, \beta$. Мы поступим так: сперва набросаем план вывода – разместим по тексту «ключевые» формулы, которые потом дополним до полноценного вывода промежуточными формулами. Формулы в плане занумеруем через 10, чтобы иметь возможность вставлять дополнительные утверждения посередине.

План вывода будет такой:

(10)	$\Gamma \vdash \alpha \to \delta_1$
...	
$(10m-10)$	$\Gamma \vdash \alpha \to \delta_{m-1}$
$(10m)$	$\Gamma \vdash \alpha \to \beta$

Теперь надо дополнить его до полноценного вывода. Будем рассматривать формулы подряд и перед каждой формулой добавлять некоторое количество формул, обосновывающих соответствующий шаг доказательства. Рассмотрим формулу номер i. Возможны следующие варианты:

1. δ_i — это аксиома или предположение, входящее в Γ. Тогда перед этой формулой вставим формулы δ_i и $\delta_i \to (\alpha \to \delta_i)$, и окажется, что i-я формула выводится из предыдущих двух формул путем применения правила Modus Ponens.

2. δ_i совпадает с α. Тогда мы вставим перед ней 4 первые формулы из леммы, и $\delta_i \to \alpha$ будет получаться по правилу Modus Ponens.

3. δ_i выводится по правилу Modus Ponens из каких-то других утверждений δ_j и δ_k (которое есть $\delta_j \to \delta_i$), где $j, k < i$. Покажем, что $\alpha \to \delta_i$ тоже может быть выведена из утверждений $\alpha \to \delta_j$ и $\alpha \to (\delta_j \to \delta_i)$.

   Для этого добавим два высказывания:

$(i-6)$	$(\alpha \to \delta_i) \to ((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	Сх. акс. 2
$(i-3)$	$((\alpha \to (\delta_j \to \delta_i)) \to (\alpha \to \delta_i))$	М.Р. из j и $i-6$

□

По аналогии мы можем рассмотреть отношение *следования*. Будем говорить, что высказывание α следует из высказываний Γ, если при любой оценке пропозициональных переменных, входящих в высказывания Γ и α, на которых все высказывания из Γ истинны, α также истинно. Записывать, что α следует из Γ, будем так: $\Gamma \models \alpha$.

5 Теорема о полноте исчисления высказываний

Лемма 5.1. Если $\Gamma \vdash \alpha$, то $\Gamma, \gamma \vdash \alpha$. Если $\Gamma_1, \Gamma_2 \vdash \alpha$, то $\Gamma_2, \Gamma_1 \vdash \alpha$. Аналогично для следствия.

Доказательство. Упражнение. □

Возьмем некоторую связку исчисления высказываний, например конъюнкцию: $A\&B$. Построим для нее таблицу истинности. По каждой строчке построим утверждение, в котором отрицания появляются там, где в таблице истинности находится *Л*:

A	B	$A\&B$	утверждение
Л	Л	Л	$\neg A, \neg B \vdash \neg(A\&B)$
Л	И	Л	$\neg A, B \vdash \neg(A\&B)$
И	Л	Л	$A, \neg B \vdash \neg(A\&B)$
И	И	И	$A, B \vdash A\&B$

Лемма 5.2. Так построенные по таблицам истинности утверждения верны.

Доказательство. Упражнение. □

Лемма 5.3. Правило контрапозиции.Каковы бы ни были формулы α и β, справедливо, что $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

Доказательство. Сперва докажем, что $\alpha \to \beta, \neg\beta \vdash \neg\alpha$.

(1)	$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$	Сх. акс. 8
(2)	$\alpha \to \beta$	Допущение
(3)	$(\alpha \to \neg\beta) \to \neg\alpha$	М.Р. 2,1
(4)	$\neg\beta \to (\alpha \to \neg\beta)$	Сх. акс. 1
(5)	$\neg\beta$	Допущение
(6)	$\alpha \to \neg\beta$	М.Р. 5,4
(7)	$\neg\alpha$	М.Р. 6,3
(1)	$\alpha \to \neg\neg\beta, \alpha \vdash \alpha \to \neg\neg\beta$	

Тогда, применив 2 раза Теорему о дедукции, получим вывод требуемого утверждения.

□

Лемма 5.4. Правило исключенного третьего. Какова бы ни была формула α, $\vdash \alpha \vee \neg\alpha$

Доказательство. Доказательство проведем в 3 этапа.

1. Для начала покажем $\vdash \neg(\alpha \vee \neg\alpha) \to \neg\alpha$:

(1)	$\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 6
(2)	$(\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\alpha)$	по лемме 5.3
(3)	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	М.Р. 1,2

2. Доказательство $\vdash \neg(\alpha \vee \neg\alpha) \to \alpha$ чуть сложнее:

(1)	$\neg\alpha \to \alpha \vee \neg\alpha$	Сх. акс. 7
(2)	$(\neg\alpha \to \alpha \vee \neg\alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha)$	по лемме 5.3
(3)	$\neg(\alpha \vee \neg\alpha) \to \neg\neg\alpha$	М.Р. 1,2

Применив обратную теорему о дедукции, получим: $\neg(\alpha\vee\neg\alpha) \vdash \neg\neg\alpha$. Далее, в данном допущении, построим следующий вывод:

(1)	$\neg\neg\alpha \to \alpha$	Сх. акс. 10
(2)	$\neg\neg\alpha$	Доказуемо при допущении $\neg(\alpha \vee \neg\alpha)$
(3)	α	М.Р. 2,1

И по теореме о дедукции из данного вывода мы можем получить доказательство утверждения $\vdash \neg(\alpha \vee \neg\alpha) \to \alpha$.

3. Теперь докажем все вместе:

(1)	$\neg(\alpha \vee \neg\alpha) \to \neg\alpha$	по пункту 1
(2)	$\neg(\alpha \vee \neg\alpha) \to \alpha$	по пункту 2
(3)	$(\neg(\alpha \vee \neg\alpha) \to \alpha) \to (\neg(\alpha \vee \neg\alpha) \to \neg\alpha) \to (\neg\neg(\alpha \vee \neg\alpha))$	Сх. акс. 9
(4)	$(\neg(\alpha \vee \neg\alpha) \to \neg\alpha) \to \neg\neg(\alpha \vee \neg\alpha)$	М.Р. 2,3
(5)	$\neg\neg(\alpha \vee \neg\alpha)$	М.Р. 1,4
(6)	$\neg\neg(\alpha \vee \neg\alpha) \to (\alpha \vee \neg\alpha)$	Сх. акс. 10
(7)	$\alpha \vee \neg\alpha$	М.Р. 5,6

□

Теорема 5.5. Пусть справедливо $\models \alpha$. Тогда также справедливо, что $\vdash \alpha$.

Доказательство. См. Стефан Клини, Математическая логика, М. «Мир», 1973. Глава 1, параграф 12, стр. 61-64. □

6 Исчисление предикатов

Выберем множество истинностных значений V. Также, выберем некоторое предметное множество D. *n-местным предикатом* мы назовем функцию из D^n в V. Как и раньше, мы ограничимся классическим множеством V – истина и ложь, но оставляем потенциальную возможность его расширить.

Предикаты могут быть 0-местными, в этом случае это хорошо нам известные пропозициональные переменные, принимающие какие-то истинностные значения, в происхождение которых мы не вникаем.

Рассмотрим следующий известный пример: каждый человек смертен, Сократ - человек, следовательно, Сократ - смертен. Мы можем формализовать это выражение с помощью предикатов: множество D - это будет множество всех существ, $S(x)$ - предикат «быть смертным», $H(x)$ - предикат «быть человеком». Тогда фраза в полу-формальном виде выглядит так: Для каждого x, такого, что $H(x)$ верно $S(x)$, поэтому поскольку H(Сократ), значит, что имеет место S(Сократ).

Чтобы построить новое исчисление, нам требуется указать 3 компонента: язык, аксиомы и правила вывода.

1. Язык. Добавим к языку исчисления высказываний новые конструкции с предикатами и получим язык исчисления предикатов. Вот расширенная грамматика:

```
 <выражение>  ::=  <импликация>
<импликация>  ::=  <дизъюнкция> | <дизъюнкция> → <импликация>
<дизъюнкция>  ::=  <конъюнкция> | <дизъюнкция> ∨ <конъюнкция>
<конъюнкция>  ::=  <терм> | <конъюнкция>&<терм>
      <терм>  ::=  <предикат> | <предикат> (<аргументы>)
               |   (<выражение>)
               |   ∃<переменная><терм> | ∀<переменная><терм>
 <аргументы>  ::=  <переменная>
 <аргументы>  ::=  <переменная>,<аргументы>
```

   Добавились 3 новых сущности:

   (a) *индивидные* переменные — мы будем записывать их маленькими латинскими буквами из начала алфавита

   (b) предикаты (они обобщили пропозициональные переменные)

   (c) кванторы: всеобщности ($\forall$) и существования ($\exists$).

2. Аксиомы.

   Определение 6.1. Дана некоторая формула s. Будем говорить, что подстрока s_1 строки s является подформулой, если она в точности соответствует какому-то одному нетерминалу в дереве разбора строки s.

   Определение 6.2. Если в формулу входит подформула, полученная по правилам для кванторов (то есть, $\forall x\alpha$ или $\exists x\alpha$), то мы будем говорить, что формула α находится в области действия данного квантора по переменной x. Также, будем говорить, что любая подформула формулы α находится в области действия данного квантора.

Определение 6.3. Если некоторое вхождение переменной x находится в области действия квантора по переменной x, то такое вхождение мы назовем *связанным*. Вхождение переменной x непосредственно рядом с квантором $(\forall x \ldots)$ мы назовем *связывающим*. Те вхождения переменных, которые не являются связанными или связывающими, назовем *свободными*. Формула, не имеющая свободных вхождений переменных, называется *замкнутой*.

Определение 6.4. Будем говорить, что переменная y свободна для x при подстановке в формулу ψ (или просто свободна для подстановки вместо x), если после подстановки y вместо свободных вхождений x ни одно ее вхождение не станет связанным.

Чтобы получить список аксиом для исчисления предикатов, возьмем все схемы аксиом исчисления высказываний и дополним их следующими двумя схемами. Здесь x - переменная, ψ - некоторая формула, y - некоторая переменная. Запись $\psi[x := y]$ будет означать результат подстановки y в ψ вместо всех свободных вхождений x. Пусть y свободно для подстановки вместо x.

(11) $\forall x(\psi) \to (\psi[x := \alpha])$
(12) $(\psi[x := \alpha]) \to \exists x(\psi)$

Заметим, что если взять формулу $\exists x A(x, y)$, то по схеме аксиом (11), если игнорировать ограничение на свободу для подстановки, следующее утверждение должно быть тавталогией: $\forall y \exists x A(x, y) \to \exists x A(x, x)$. Однако, оно ей не является.

Все аксиомы, порожденные данными схемами в новом языке, мы назовем аксиомами исчисления предикатов.

3. Правила вывода.

   Пусть x не входит свободно в ϕ. Тогда рассмотрим следующие дополнительные правила вывода исчисления предикатов:

   $$\frac{(\phi) \to (\psi)}{(\phi) \to \forall x(\psi)} \quad \frac{(\psi) \to (\phi)}{\exists x(\psi) \to (\phi)}$$

   Добавив эти схемы к схеме для правила Modus ponens исчисления высказываний, мы сможем породить множество правил вывода.

Определение 6.5. Формальная система, составленная из указанного языка, множества аксиом и множества правил вывода, называется исчислением предикатов.

Для задания оценки для выражения в исчислении предикатов необходимо вместо оценки для переменных f_P в исчислении высказываний ввести оценку для предикатов: для каждого k-местного предиката P_n^k определить функцию $f_{P_n^k} : D^k \to V$.

Определение 6.6. Формула в исчислении предикатов общезначима, если она истинна на любом предметном множестве D, при любой оценке предикатов, и при любых оценках свободных индивидных переменных.

Определение 6.7. Пусть имеется некоторое исчисление предикатов с множеством аксиом A, и пусть дан некоторый (возможно, пустой) список Γ *замкнутых* формул исчисления предикатов. Тогда, вывод формулы α в исчислении с аксиомами $A \cup \Gamma$ мы назовем выводом из допущений Γ, и будем записывать это как $\Gamma \vdash \alpha$.

Обратите внимание на требование отсутствия свободных переменных в допущениях.

Теорема 6.1. Исчисление предикатов корректно, т.е. любое доказуемое утверждение общезначимо.

Доказательство. Упражнение. $\square$

Теорема 6.2. Теорема о дедукции. Если $\Gamma, \alpha \vdash \beta$, то $\Gamma \vdash \alpha \to \beta$

Доказательство. Доказательство разбором случаев. 3 старых случая те же, добавилось 2 новых правила вывода. Упражнение. $\square$

Теорема 6.3. Исчисление предикатов полно.

Без доказательства.

7 Секвенциальное исчисление высказываний

Исчисления гильбертовского типа, используемые здесь, не единственные. Как пример, рассмотрим секвенциальное исчисление. В данном разделе мы будем использовать символ $\supset$ вместо символа $\rightarrow$.

Определение 7.1. Пусть Γ и Δ — некоторые списки формул исчисления высказываний. Тогда секвенция — это запись вида $\Gamma \rightarrow \Delta$. Часть секвенции слева от символа ($\rightarrow$) называется *антецедентом*, а справа — *сукцедентом*

Неформальный смысл секвенции: секвенция $\gamma_1, ...\gamma_n \rightarrow \delta_1, ...\delta_n$ означает, что из конъюнкции всех аргументов слева следует дизъюнкция всех аргументов справа. Пустой список слева соответствует истине, пустой список справа — лжи. Соответственно, доказуемость секвенции $\rightarrow$ означает противоречие.

Формальная система, основанная на секвенциальном исчислении, имеет одну схему аксиом: $(\psi) \rightarrow (\psi)$, и множество правил вывода.

Правила вывода и аксиомы смотри в книге Г. Такеути Теория доказательств, М, «Мир», 1978, стр. 15-17.

Теорема 7.1. Теорема об устранении сечений. Любое доказательство, использующее правило сечения, может быть перестроено в доказательство, не использующее правило сечения.

Без доказательства.

Интуиционистское исчисление высказываний может быть получено из классического путем введения ограничения на количество формул в сукцеденте: их должно быть не более одной.

8 Интуиционистская логика

Интуиционистское исчисление высказываний получается из классического заменой схемы аксиом 10 в исчислении высказываний (схемы аксиом снятия двойного отрицания) на следующую:

$$(\neg(\psi)) \rightarrow (\psi) \rightarrow (\phi)$$

Конструкцию примера для доказательства необщезначимости закона исключенного третьего и конструкцию моделей Крипке см. Н.К.Шень, А.Верещагин, Лекции по математической логике и теории алгоритмов, часть 2. Языки и Исчисления.
`http://www.mccme.ru/free-books/shen/shen-logic-part2.pdf`
Глава 2, Интуиционистская пропозициональная логика, стр. 74-77.

9 Теории первого порядка

Мы занимались до этого момента только логическими рассуждениями самими по себе. Это интересно, но не очень практически полезно: мы все-таки используем логические рассуждения для доказательства утверждений о каких-то объектах. Было бы разумно каким-то образом включить эти объекты в рамки формальной теории.

Рассмотрим некоторое множество N. Будем говорить, что оно удовлетворяет аксиомам Пеано, если выполнено следующее:

- В нем существует некоторый выделенный элемент 0.
- Для каждого элемента множества определена операция $'$.

Кроме того, эти элемент и операция должны удовлетворять следующим требованиям:

- Не существует такого x, что $x' = 0$.
- Если $x' = y'$, то $x = y$.
- Если некоторое предположение верно для 0, и если из допущения его для n можно вывести его истинность для $n + 1$, то предположение верно для любого элемента множества.

Данная аксиоматика позволяет определить натуральные числа (множество натуральных чисел — это множество, удовлетворяющее аксиомам Пеано; заметим, что тут натуральные числа содержат 0, так оказывается удобнее) и операции над ними. Например, сложение можно задать следующими уравнениями:

$$a + 0 = a$$
$$a + b' = (a + b)'$$

Теорема 9.1. Так определенное сложение коммутативно.

Доказательство. Упражнение. □

Но данная аксиоматика сформулирована неформально, поэтому мы не сможем доказать никаких содержательных утверждений про нее, пользуясь формальными средствами. Поэтому нам нужно эту конструкцию как-то объединить с исчислением предикатов, чем мы сейчас и займемся.

Рассмотрим следующее исчисление. Мы уже не будем приводить грамматику, ожидая, что это является простым упражнением, приведем только общее описание.

Возьмем язык исчисления предикатов со следующими изменениями и особенностями:

- Маленькими латинскими буквами a,b,... (возможно, с индексами) будем обозначать индивидные переменные.
- К логическим связкам добавляются такие: $(=)$ — двуместный предикат, $(+)$ и $(\cdot)$ — двуместные функции, и $(')$ — одноместная функция. Все левоассоциативное, приоритеты в порядке убывания: $(')$, потом $(\cdot)$, потом $(+)$. Все логические связки имеют приоритет ниже. Например, $a = b' + b' + c \cdot c \& b = c$ надо интерпретировать как $(a = (((b') + (b')) + (c \cdot c))) \& (b = c)$.
- Вводится 0-местная функция 0.

Ранее мы для простоты не рассматривали функции в исчислении предикатов, но здесь без них уже не обойтись. Функции, в отличие от предикатов, имеют своей областью значений предметное множество, то есть в качестве аргумента предикатов в таком исчислении можно писать не только переменные, но и произвольные выражения из переменных и применения функций. Функции нетрудно формализовать, добавив дополнительные правила к грамматике и расширив логические схемы аксиом (11) и (12), разрешив в них заменять индивидную переменную не только на другую переменную, но и на произвольное выражение из функций и переменных.

К стандартным аксиомам исчисления предикатов добавим следующие 8 *нелогических* аксиом и одну нелогическую схему аксиом.

(A1) $a = b \to a' = b'$
(A2) $a = b \to a = c \to b = c$
(A3) $a' = b' \to a = b$
(A4) $\neg a' = 0$
(A5) $a + b' = (a + b)'$
(A6) $a + 0 = a$
(A7) $a \cdot 0 = 0$
(A8) $a \cdot b' = a \cdot b + a$
(A9) $(\psi[x := 0])\&\forall x((\psi) \to (\psi)[x := x']) \to (\psi)$

В схеме аксиом (A9) ψ – некоторая формула исчисления предикатов и x — некоторая переменная, входящая свободно в ψ.

Теорема 9.2. $\vdash a = a$

Доказательство. Упражнение. Клини, стр. 254. □

Определение 9.1. Структура. Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P\rangle$, где $F = \langle F_0, F_1, ...\rangle$ — списки оценок для 0-местных, 1-местных и т.д. функций, и $P = \langle P_0, P_1, ...\rangle$ — списки оценок для 0-местных, 1-местных и т.д. предикатов, D — предметное множество.

Понятие структуры — развитие понятия оценки из исчисления предикатов. Но оно касается только нелогических составляющих теории; истинностные значения и оценки для связок по-прежнему определяются исчислением предикатов, лежащим в основе теории. Для получения оценки формулы нам нужно задать структуру, значения всех свободных индивидных переменных, и (естественным образом) вычислить результат.

Определение 9.2. Назовем структуру корректной, если любая доказуемая формула истинна в данной структуре.

Определение 9.3. Моделью теории мы назовем любую корректную структуру.

Еще одним примером теории первого порядка может являться теория групп. К исчислению предикатов добавим двуместный предикат $(=)$, двуместную функцию $(\cdot)$, одноместную функцию (x^{-1}), константу (т.е. 0-местную функцию) 1 и следующие аксиомы:

(E1) $a = b \to (a = c \to b = c)$
(E2) $a = b \to (a \cdot c = b \cdot c)$
(E3) $a = b \to (c \cdot a = c \cdot b)$
(G1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(G2) $a \cdot 1 = a$
(G3) $a \cdot a^{-1} = 1$

Теорема 9.3. Доказуемо, что $a = b \to b = a$ и что $a^{-1} \cdot a = 1$.

Доказательство. Упражнение. □

Определение 9.4. Назовем модели некоторой теории первого порядка с предметными множествами D_1 и D_2 изоморфными, если существует биективная функция $I : D_1 \to D_2$, при этом для любой функции f данной теории, имеющей оценки f_1 и f_2 (в первой и второй модели соответственно) и любых $x_1, ...x_n$ из D_1 справедливо $f_2(I(x_1), ...I(x_n)) = I(f_1(x_1, ...x_n))$ и для любого предиката P (P_1 и P_2 определены аналогично) $P_2(I(x_1), ...I(x_n))$ тогда и только тогда, когда $P_1(x_1, ...x_n)$.

Теорема 9.4. Существуют неизоморфные модели для теории групп, имеющие конечные предметные множества равной мощности.

Доказательство. Упражнение. □

10 Рекурсивные функции.

Рассмотрим примитивы, из которых будем собирать выражения:

1. $Z : N \to N$, $Z(x) = 0$
2. $N : N \to N$, $N(x) = x'$
3. Проекция. $U_i^n : N^n \to N$, $U_i^n(x_1, ...x_n) = x_i$
4. Подстановка. Если $f : N^n \to N$ и $g_1, ...g_n : N^m \to N$, то $S\langle f, g_1, ...g_n\rangle : N^m \to N$. При этом $S\langle f, g_1, ...g_n\rangle(x_1, ...x_m) = f(g_1(x_1, ...x_m), ...g_n(x_1, ...x_m))$
5. Примитивная рекурсия. Если $f : N^n \to N$ и $g : N^{n+2} \to N$, то $R\langle f, g\rangle : N^{n+1} \to N$, при этом

$$R\langle f, g\rangle(x_1, ...x_n, y) = \begin{cases} f(x_1, ...x_n) & , y = 0 \\ g(x_1, ...x_n, y - 1, R\langle f, g\rangle(x_1, ...x_n, y - 1)) & , y > 0 \end{cases}$$

6. Минимизация. Если $f : N^{n+1} \to N$, то $\mu\langle f\rangle : N^n \to N$, при этом $\mu\langle f\rangle(x_1, ...x_n)$ — такое минимальное число y, что $f(x_1, ...x_n, y) = 0$. Если такого y нет, результат данного примитива неопределен.

Если некоторая функция $N^n \to N$ может быть задана с помощью данных примитивов, то она называется рекурсивной. Если некоторую функцию можно собрать исключительно из первых 5 примитивов (то есть без использования операции минимизации), то такая функция называется примитивно-рекурсивной.

Теорема 10.1. Следующие функции являются примитивно-рекурсивными: сложение, умножение, ограниченное вычитание (которое равно 0, если результат вычитания отрицателен), целочисленное деление, остаток от деления.

Доказательство. Упражнение. □

11 Арифметические функции и отношения. Их выразимость в формальной арифметике.

Введем обозначение. Будем говорить, что $\alpha(x_1, \dots x_n)$ — это формула с n свободными переменными, если переменные $x_1, ...x_n$ входят в α свободно. Запись $\alpha(y_1, \dots y_n)$ будем трактовать, как $\alpha[x_1 := y_1, ...x_n := y_n]$, при этом мы подразумеваем, что $y_1, \dots y_n$ свободны для подстановки вместо $x_1, \dots x_n$ в α.

Также, запись $B(x_1, \dots x_n) := \alpha(x_1, \dots x_n)$ будет означать, что мы определяем новую формулу с именем B. Данная формула должна восприниматься только как сокращение записи, макроподстановка.

Определение 11.1. Арифметическая функция — функция $f : N^n \to N$. Арифметическое отношение — n-арное отношение, заданное на N.

Определение 11.2. Арифметическое отношение R называется выразимым (в формальной арифметике), если существует такая формула $\alpha(x_1, \dots x_n)$ с n свободными переменными, что для любых натуральных чисел k_1 ... k_n

1. если $R(k_1, \dots k_n)$ истинно, то доказуемо $\alpha(\overline{k_1}, \dots \overline{k_n})$

2. если $R(k_1, \dots k_n)$ ложно, то доказуемо $\neg\alpha(\overline{k_1}, \dots \overline{k_n})$.

Например, отношение ($<$) является выразимым в арифметике: Рассмотрим формулу $\alpha(a_1, a_2) = \exists b(\neg b = 0 \& a_1 + b = a_2)$. В самом деле, если взять некоторые числа k_1 и k_2, такие, что $k_1 < k_2$, то найдется такое положительное число b, что $k_1 + b = k_2$. Можно показать, что если подставить $\overline{k_1}$ и $\overline{k_2}$ в α, то формула будет доказуема.

Наметим доказательство: Тут должно быть два доказательства по индукции, сперва по k_2, потом по k_1. Рассмотрим доказательство по индукции: пусть $k_1 = 0$, индукция по 2-му параметру: Разберем доказательство базы при $k_2 = 1$. Тогда надо показать $\exists b(\neg b = 0 \& 0 + b = 1)$:

(1)	$\neg 1 = 0 \& 0 + 1 = 1$	Несложно показать
(2)	$(\neg 1 = 0 \& 0 + 1 = 1) \to \exists b(\neg b = 0 \& 0 + b = 1)$	Сх. акс. для $\exists$
(3)	$\exists b(\neg b = 0 \& 0 + b = 1)$	M.P. 1 и 2.

Определение 11.3. Введем следующее сокращение записи: пусть $\exists! y \phi(y)$ означает

$$\exists y \phi(y) \& \forall a \forall b(\phi(a) \& \phi(b) \to a = b)$$

Здесь a и b — некоторые переменные, не входящие в формулу ϕ свободно.

Определение 11.4. Арифметическая функция f от n аргументов называется представимой в формальной арифметике, если существует такая формула $\alpha(x_1, \dots x_{n+1})$ с $n+1$ свободными пременными, что для любых натуральных чисел k_1 ... k_n

1. $f(k_1, \dots k_n) = k_{n+1}$ тогда и только тогда, когда доказуемо $\alpha(\overline{k_1}, \dots \overline{k_{n+1}})$.
2. Доказуемо $\exists! b(\alpha(\overline{k_1}, \dots \overline{k_n}, b)$

Теорема 11.1. Функции Z, N, U_i^n являются представимыми.

Доказательство. Наметим доказательство. Для этого приведем формулы, доказательство корректности этих формул оставим в виде упражнения.

- Примитив Z представит формула $Z(a, b) := (a = a \& b = 0)$.
- Примитив N представит формула $N(a, b) := (a' = b)$.
- Примитив U_i^n представит формула $U_i^n(a_1, ...a_n, b) = (a_1 = a_1) \& ... \& (a_n = a_n) \& (b = a_i)$.

□

Теорема 11.2. Если функции f и g_1, ... g_m представимы, то функция $S\langle f, g_1, \dots g_m \rangle$ также представима.

Доказательство. Поскольку функции f и g_i представимы, то есть формулы F и $G_1, \dots G_m$, их представляющие. Тогда следующая формула представит $S\langle f, g_1, \dots g_m \rangle$:

$$S(a_1, \dots a_n, b) := \exists b_1 \dots \exists b_m (G_1(a_1, \dots a_n, b_1) \& \dots \& G_m(a_1, \dots a_n, b_m) \& F(b_1, \dots b_m, b))$$

□

Определение 11.5. Характеристическая функция арифметического отношения R — это функция

$$C_R(x_1, ...x_n) = \begin{cases} 0 & R(x_1, ...x_n) \\ 1 & R(x_1, ...x_n) \text{ неверно} \end{cases}$$

Очевидно, что характеристическая функция представима тогда и только тогда, когда отношение выразимо.

Определение 11.6. β-функция Геделя - это функция $\beta(b, c, i) = b\%(1 + c \cdot (i + 1))$. Здесь операция ($\%$) означает взятие остатка от целочисленного деления.

Лемма 11.3. Функция примитивно-рекурсивна, и при этом представима в арифметике формулой $B(b, c, i, d) := \exists q((b = q \cdot (1 + c \cdot (i + 1)) + d)\&(d < 1 + c \cdot (i + 1)))$

Доказательство. Упражнение. □

Лемма 11.4. Для любой конечной последовательности чисел k_0 ... k_n можно подобрать такие константы b и c, что $\beta(b, c, i) = k_i$ для $0 \leq i \leq n$.

Доказательство. Возьмем число $c = max(k_1, \dots k_n, n)!$. Рассмотрим числа $u_i = 1+c\cdot(i+1)$.

- Никакие числа u_i и u_j $(0 \leq j < i \leq n)$ не имеют общих делителей кроме 1. Пусть это не так, и есть некоторый общий делитель p (очевидно, мы можем предположить его простоту — разложив на множители, если он составной). Тогда p будет делить $u_i - u_j = c\cdot(i-j)$, при этом p не может делить c — иначе окажется, что $u_i = (1+c\cdot(i+1))$ делится на p и $c \cdot (i + 1)$ делится на p. Значит, p делит $i - j$, то есть все равно делит c, так как c — факториал некоторого числа, не меньшего n, и при этом $i - j \leq n$.

- Каждое из чисел k_i меньше, чем u_i: в самом деле, $k_i \leq c < 1 + c \cdot (i + 1) = u_i$.

- Согласно китайской теореме об остатках, если некоторые натуральные числа $k_0, \dots k_n$ попарно взаимно просты, то для любых целых чисел $u_0, \dots u_n$, таких, что $0 \leq k_i < u_i$, найдется такое целое число b, для которого выполнено $k_i = b\%u_i$. Возьмем b, подсказываемое теоремой об остатках.

□

Теорема 11.5. Всякая рекурсивная функция представима в арифметике.

Доказательство. Представимость первых четырех примитивов уже показана. Покажем представимость примитивной рекурсии и операции минимизации.

Примитивная рекурсия. Пусть есть некоторый $R\langle f, g\rangle$. Соответственно, f и g уже представлены как некоторые формулы F и G. Из определения $R\langle f, g\rangle$ мы знаем, что для значения $R\langle f, g\rangle(x_1, ...x_{n+1})$ должна существовать последовательность $a_0...a_{x_{n+1}}$ результатов применения функций f и g — значений на одно больше, чем итераций в цикле примитивной рекурсии, а это количество определяется последним параметром функции $R\langle f, g\rangle$. При этом:

$a_0 = f(x_1, \dots x_n)$
$a_1 = g(x_1, \dots x_n, 0, a_0)$
...
$a_{x_{n+1}} = g(x_1, \dots x_n, x_{n+1} - 1, a_{x_{n+1}-1})$

Значит, по лемме, должны существовать такие числа b и c, что $\beta(b, c, i) = a_i$ для $0 \leq i \leq x_{n+1}$.

Приведенные рассуждения позволяют построить следующую формулу, представляющую $R\langle f, g\rangle(x_1, ...x_{n+1})$:

$$\begin{gathered} R(x_1, \dots x_{n+1}, a) := \exists b \exists c(\exists k(B(b, c, 0, k)\&F(x_1, ...x_n, k)) \\ \&B(b, c, x_{n+1}, a) \\ \&\forall k(k < x_{n+1} \to \exists d \exists e(B(b, c, k, d)\&B(b, c, k', e)\&G(x_1, ..x_n, k, d, e))) \end{gathered}$$

Минимизация. Рассмотрим конструкцию $\mu\langle f\rangle$. f уже представлено как некоторая формула F. Тогда формула $M(x_1, \dots x_n, y) := F(x_1, \dots x_n, y, 0) \& \forall z(z < y \to \neg F(x_1, \dots x_n, z, 0))$ представит $\mu\langle f\rangle$.

$\square$

12 Геделева нумерация. Арифметизация доказательств

Ранее мы показали, что любое рекурсивное арифметическое отношение выразимо в формальной арифметике. Теперь мы покажем, что наоборот, любое выразимое в формальной арифметике отношение является рекурсивным.

Определение 12.1. Ограниченные кванторы $\exists_{x<y}\phi(x)$ и $\forall_{x<y}\phi(x)$ — сокращения записи для выражений вида $\exists x(x < y \& \phi(x))$ и $\forall x(x \geq y \vee \phi(x))$

Теорема 12.1. Пусть P_1 и P_2 — рекурсивные отношения. Тогда следующие формулы, задающие некоторые отношения, также являются рекурсивными отношениями:

1. $F(x_1, \dots x_n, z) := \forall_{y<z} P_1(x_1, \dots x_n, y)$
2. $E(x_1, \dots x_n, z) := \exists_{y<z} P_1(x_1, \dots x_n, y)$
3. $P_1(x_1, \dots x_n) \to P_2(x_1, \dots x_n)$
4. $P_1(x_1, \dots x_n) \vee P_2(x_1, \dots x_n)$
5. $P_1(x_1, \dots x_n) \& P_2(x_1, \dots x_n)$
6. $\neg P_1(x_1, \dots x_n)$

Доказательство. Упражнение. □

Теперь мы перенесем понятие вывода формулы на язык рекурсивных отношений, и, следовательно, внутрь языка формальной арифметики.

Определение 12.2. Геделева нумерация.Дадим следующие номера символам языка формальной арифметики:

3	(	
5	)	
7	,	
9	$\neg$	
11	$\to$	
13	$\vee$	
15	&	
17	$\forall$	
19	$\exists$	
$13 + 8 \cdot k$	x_k	переменные
$15 + 8 \cdot k$	a_k	константы
$17 + 8 \cdot 2^k \cdot 3^n$	f_k^n	n-местные функциональные символы: ($'$), (+) и т.п.
$19 + 8 \cdot 2^k \cdot 3^n$	P_k^n	n-местные предикаты, в т.ч. (=)

Уточним язык — обяжем всегда писать скобки всегда и только вокруг двуместной операции. В принципе, иначе мы могли бы определить правильно операцию равенства Eq, но это лишние технические сложности.

Научимся записывать выражения в виде чисел. Пусть $p_1, \dots p_k, \dots$ — список простых чисел, при этом $p_1 = 2, p_2 = 3, \dots$.

Тогда текст из n символов с геделевыми номерами $c_1, \dots c_n$ запишем как число $t = p_1^{c_1} \cdot p_2^{c_2} \cdot \dots \cdot p_n^{c_n}$. Ясно, что такое представление однозначно позволяет установить длину строки (геделева нумерация не содержит 0, поэтому можно определить длину строки как максимальный номер простого числа, на которое делится t; будем записывать эту функцию как $Len(s)$), и каждый символ строки в отдельности (будем записывать функцию как $(s)_n$). Также ясно, что функции Len и $(x)_n$ — рекурсивны.

Чтобы удобнее работать со строками, введем следующую запись. Пусть есть запись вида «$_1c_2c_3\dots$», здесь c_i — какие-то символы языка формальной арифметики, заключенные в кавычки. Эта запись задает число $p_1^{c_1}\cdot\ldots\cdot p_n^{c_n}$.

Операцию конкатенации строк $s \star t$ определим так. Пусть первая строка имеет символы $s_1,\dots s_n$, а вторая — $t_1,\dots t_m$. Тогда результат их конкатенации — $p_1^{s_1}\cdot\ldots\cdot p_n^{s_n}\cdot p_{n+1}^{t_1}\cdot\ldots\cdot p_{n+m}^{t_m}$.

Если в данной записи встретится символ с \$ перед ним: «$\neg\$x\&y$», тогда это означает вставку «литерала» (ср. язык Perl) — интерпретировать это надо как конкатенацию строки до литерала, самого литерала, и строки после литерала. В данном примере — «$\neg$»$\star x\star$«$\&y$».

Чтобы представить доказательства, мы будем объединять строки вместе так же, как объединяем символы в строки: $2^{2^3}\cdot 3^{2^5}$ — это последовательность из двух строк, первая — это «(», а вторая — «)».

Теперь мы можем понять, как написать программу, проверяющую корректность доказательства некоторого утверждения в формальной арифметике. Наметим общую идею. Программа будет состоять из набора рекурсивных отношений и функций, каждое из которых выражает некоторое отношение, содержательное для проверки доказательства. Ниже мы покажем идею данной конструкции, приведя несколько из них.

- Проверка того, что a - геделев номер выражения, являющегося переменной. $Var(a) := \exists_{z<a}(a = 2^{13+z})$
- Проверка того, что выражение с номером a получено из выражений b и c путем применения правила Modus Ponens. $MP(b,c,a) := c =$«(\$$b \to$ \$$a$)»
- Проверка того, что b получается из a подстановкой y вместо x: $Subst(a,b,x,y)$ — без реализации
- Функция, подставляющая y вместо x в формуле a:
$Sub(a,x,y) := \mu\langle S\langle Subst, U_1^4, U_4^4, U_2^4, U_3^4\rangle\rangle(a,x,y)$
- Проверка того, что переменная x входит свободно в формулу f.
$Free(f,x) := \neg Subst(a,a,x,13+8^x)$
- Функция, выдающая геделев номер выражения, соответствующего целому числу:
$Num(n) := R\langle$«0»,«\$$U_3^{3\prime}$»$\rangle(n,n)$

Путем некоторых усилий мы можем выписать формулу, представляющую двуместное отношение $Proof(f,p)$, истинное тогда и только тогда, когда p — геделев номер доказательства формулы с геделевым номером f.

Теорема 12.2. Любая представимая в формальной арифметике функция является рекурсивной.

Доказательство. Возьмем некоторую представимую функцию $f : N^n \to N$. Значит, для нее существует формула формальной арифметики, представляющая ее. Пусть F — эта формула (со свободными переменными $x_1,\dots x_n,y$); при этом в случае $f(u_1,\dots u_n) = v$ должно быть доказуемо $F(\overline{u_1},\dots\overline{u_n},\overline{v})$. По формуле можно построить рекурсивную функцию, $C_F(u_1,\dots u_n,v,p)$, выражающую тот факт, что p — геделев номер вывода формулы $F(\overline{u_1},\dots\overline{u_n},\overline{v})$. Тогда возьмем

$$f(x_1,\dots x_n) := (\mu\langle S\langle C_F, U_1^{n+1},\dots U_n^{n+1},(U_{n+1}^{n+1})_1,(U_{n+1}^{n+1})_2)\rangle\rangle(x_1,\dots x_n))_1$$

. $\square$

13 1я и 2я теоремы Геделя о неполноте арифметики

Определение 13.1. Мы будем называть теорию непротиворечивой, если не найдется такой формулы F, что доказуемо как F, так и $\neg F$.

Лемма 13.1. Если теория противоречива, то в ней доказуемо любая формула.

Доказательство. Если теория противоречива, то в ней есть утверждение F, что доказуемо F и $\neg F$. Воспользуемся доказуемой формулой $\neg F \to F \to \beta$. □

Определение 13.2. Мы будем называть теорию ω-непротиворечивой, если, какова бы ни была формула $P(x)$ со свободной переменной x, такая, что для любого натурального числа p доказуемо $P(p)$, то формула $\exists p \neg P(p)$ недоказуема.

Лемма 13.2. ω-непротиворечивость влечет непротиворечивость.

Доказательство. Рассмотрим выводимую формулу $x = x \to x = x$. При подстановке любого натурального числа вместо x формула будет по-прежнему выводима: $\overline{k} = \overline{k} \to \overline{k} = \overline{k}$. Значит, по ω-непротиворечивости формула $\exists p \neg (x = x \to x = x)$ невыводима. Значит, теория непротиворечива (поскольку в противоречивой теории выводится любая формула). □

Пусть формула F со свободной переменной «x» имеет геделев номер f. Тогда определим рекурсивное отношение W_1, такое, что $W_1(f, p)$ истинно тогда и только тогда, когда p есть геделев номер доказательства $F(f)$, то есть доказательства самоприменения F. То есть в некотором приближении это будет формула вида:
$W_1(f, p) := Free(f, «x») \& Proof(Sub(f, «x», Num(f)), p)$.

Рассмотрим формулу $\forall p \neg W_1(f, p)$. Пусть w - ее геделев номер. Тогда рассмотрим формулу $\forall p \neg W_1(\overline{w}, p)$

Теорема 13.3. Первая теорема Геделя о неполноте арифметики.

1. Если формальная арифметика непротиворечива, то недоказуемо $\forall p \neg W_1(\overline{w}, p)$.
2. Если формальная арифметика ω-непротиворечива, то недоказуемо $\neg \forall p \neg W_1(\overline{w}, p)$.

Доказательство. 1. Пусть формула $\forall p \neg W_1(\overline{w}, p)$ доказуема. Тогда найдется геделев номер ее доказательства p, и значит $W_1(\overline{w}, \overline{p})$. С другой стороны, по схеме аксиом для квантора всеобщности и правилу Modus Ponens из предположения можно показать $\neg W_1(\overline{w}, \overline{p})$. Значит, получается, что формальная арифметика противоречива, что не соответствует предположению.

2. Пусть $\vdash \neg \forall p \neg W_1(\overline{w}, p)$. Значит, $\vdash \exists p W_1(\overline{w}, p)$. Значит, по ω-непротиворечивости найдется такое натуральное число p, что $\vdash W_1(\overline{w}, \overline{p})$: иначе, если $\vdash \neg W_1(\overline{w}, \overline{p})$ для любого натурального p, то по ω-непротиворечивости $\exists p \neg\neg W_1(\overline{w}, p)$ недоказуемо (напомним, что W_1 выразимо в формальной арифметике, значит, для любой пары f и p мы должны иметь либо доказательство $W_1(\overline{f}, \overline{p})$, либо доказательство отрицания этого).

Раз найдется p, что $W_1(w, p)$, то $\vdash \forall p \neg W_1(w, p)$. А, значит, доказуемо и $\neg \exists p \neg\neg W_1(w, p)$. Значит, формальная арифметика противоречива, что невозможно в силу предположения о ее ω-непротиворечивости. □

Формула $\forall p \neg W_1(w, p)$, говоря простым языком, утверждает собственную недоказуемость. Мы показали, что эта формула (при условии ω-непротиворечивости формальной арифметики) действительно недоказуема — а, значит, верна. Таким образом, мы нашли некоторое выражение в формальной арифметике, которое истинно, но недоказуемо, и тем самым показали, что если формальная арифметика ω-непротиворечива, то она неполна.

В данном рассуждении используется сложное понятие ω-непротиворечивости, что смущает. Теорема Геделя в форме Россера снимает эту сложность.

Рассмотрим отношение $W_2(f,p)$ — f и p состоят в отношении W_2 тогда и только тогда, когда p - геделев номер доказательства *отрицания* самоприменения f (если F — формула с геделевым номером f, то p — номер доказательства $\neg F(f)$). Мы можем определить его аналогично $W_1(w,p)$.

Тогда рассмотрим такую формулу $R(a)$: $\forall x(W_1(a,x) \to \exists y(y < x \& W_2(a,y)))$. Неформальным языком она утверждает, что для любого доказательства самоприменения некоторой формулы с номером a найдется доказательство (да еще и с меньшим геделевым номером) отрицания этой формулы. Ну и по традиции применим ее к своему номеру r. Внимательное рассмотрение этой ситуации приводит к следующей теореме.

Теорема 13.4. Теорема Геделя в форме Россера. Если формальная арифметика непротиворечива, то найдется такая формула F, что как она сама, так и ее отрицание недоказуемы.

Доказательство. Обозначим геделев номер R за r. В качестве формулы F возьмем формулу $R(r)$.

Рассмотрим варианты. Пусть F доказуемо, т.е. $R(r)$ истинно, т.е. $\forall x(W_1(\overline{r},x) \to \exists y(y < x \& W_2(\overline{r},y)))$ истинно. Значит, есть такой x, что $\exists y(y < x \& W_2(\overline{r},y))$ истинно. Значит, найдется такой y, что $W_2(\overline{r},y)$, т.е., что существует опровержение r с меньшим номером. Поэтому формула $R(r)$ истинной, а значит и доказуемой, быть не может.

Пусть докауземо $\neg F$. Пусть p - геделев номер доказательства. Раз так, то $W_2(r,p)$ истинно. По непротиворечивости формальной арифметики это значит, что $W_1(r,x)$ при любом x ложно (иначе окажется, что найдутся как доказательство, так и опровержение $R(r)$). Поскольку отношение $W_1(r,x)$ выразимо в формальной арифметике, то доказуемо $\neg W_1(\overline{r},\overline{x})$ при любом x (т.е. никакой из x не является доказательством $R(r)$). Как частный случай, $\neg W_1(\overline{r},\overline{x})$ доказуемо для всех x, не превышающих p, поэтому доказуемо $\neg W_1(\overline{r},1) \& \neg W_1(\overline{r},2) \& ... \& \neg W_1(\overline{r},\overline{p})$. Отсюда можно показать доказуемость формулы $x \le p \to \neg W_1(\overline{r},x)$. Обозначим эту формулу за $P_{\le}(x)$.

Рассмотрим формулу $(x \ge p) \to \exists y(y \le x \& W_2(\overline{r},y))$ Формула утверждает следующее: «если некоторый x больше чем p, то найдется такой y, меньший x, что $W_2(r,y)$». Очевидно, что данная формула истинна, ведь если мы возьмем p в качестве такого y, то $W_2(r,p)$ истинно по предположению. Обозначим рассмотренную формулу за $P_{\ge}(x)$ и заметим, что она также доказуема.

Легко показать, что из этих утверждений и из того, что $x \le p \vee x \ge p$, можно вывести $\neg W_1(\overline{r},x) \vee \exists y(y < x \& W_2(\overline{r},y))$, а отсюда - $\forall x(W_1(\overline{r},x) \to \exists y(y < x \& W_2(\overline{r},y)))$, то есть F. Однако, мы предположили доказуемость $\neg F$, и исходя из него, вывели F, т.е. показали противоречивость формальной арифметики. Значит, $\neg F$ также недоказуемо, если арифметика непротиворечива. $\square$

Теорема 13.5. Вторая теорема Геделя о неполноте арифметики. Если в формальной арифметике удастся доказать ее непротиворечивость, то на основании этого доказательства можно построить противоречие в формальной арифметике.

Доказательство. Рассмотрим только схему доказательства. Возьмем $Consis$, некоторое утверждение, которое показывает непротиворечивость арифметики, т.е. показывает отсутствие такой формулы S, что и S и $\neg S$ доказуемы (его можно выписать: $\forall s((\forall p \neg Proof(s,p)) \vee (\forall p \neg Proof(«\neg\$s», p))))$)

Тогда рассмотрим формулу $Consis \to (\forall p \neg W_1(\overline{w},p))$. Данная формула в точности соответствует условию 1й теоремы Геделя о неполноте арифметики (если формальная арифметика непротиворечива, то $\forall p \neg W_1(\overline{w},p)$ недоказуемо; напомним, что w ведь и есть геделев номер формулы $\forall p \neg W_1(x,p)$ со свободной переменной x). Рассуждение, доказывающее

1ю теорему, можно формализовать, получив доказательство данной импликации. Теперь, если у нас будет доказательство утверждения $Consis$, то по правилу Modus Ponens мы также получаем доказательство утверждения $(\forall p \neg W_1(\overline{w}, p))$. Однако, существование такого доказательства влечет за собой противоречивость формальной арифметики. $\square$

Последним в данном разделе заметим, что данные доказательства естественно обобщаются на случай произвольной формальной теории, включающей формальную арифметику. Достаточно только расширить правила, проверяющие доказательства формул на корректность (т.е. добавить в них новые аксиомы, схемы аксиом, и правила или схемы правил вывода).

14 Теория множеств.

Теория множеств строится поверх исчисления предикатов подобно формальной арифметике. Мы добавим к исчислению предикатов один новый двуместный предикат — отношение принадлежности $\in$. Еще несколько предикатов мы выразим внутри теории множеств.

Для изучения теории множеств мы также введем новую связку в исчисление предикатов — эквивалентность. $a \leftrightarrow b := a \rightarrow b \& b \rightarrow a$.

Определение 14.1. Будем говорить, что множество x является подмножеством множества y, если любой элемент x принадлежит y. Формально: $x \subseteq y$ означает, что $\forall z (z \in x \rightarrow z \in y)$.

Определение 14.2. Принцип объемности.Два множества называются равными, если они являются подмножествами друг друга. Формально: $x = y$ означает, что $x \subseteq y \& y \subseteq x$.

Аксиома 14.1. Аксиома равенства. Равные множества содержатся в одних и тех же множествах. Формально: $\forall x \forall y \forall z (x = y \& x \in z \rightarrow y \in z)$.

Аксиома 14.2. Аксиома пары. Каковы бы ни были два различных множества x и y, существует множество, состоящее в точности из них. Будем записывать это так: $\{x, y\}$. Формально: $\forall x \forall y (\neg x = y \rightarrow \exists p (x \in p \& y \in p \& \forall z (z \in p \rightarrow (z = x \vee z = y))))$.

Аксиома 14.3. Аксиома объединения. Для любого множества x, содержащего хотя бы один элемент, найдется такое множество, которое состоит в точности из тех элементов, из которых состоят элементы x. Будем записывать это так: $\cup x$. Формально: $\forall x (\exists y y \in x \rightarrow \exists p \forall y (y \in p \leftrightarrow \exists s (y \in s \& s \in x)))$

Аксиома 14.4. Аксиома степени. Каково бы ни было множество x, существует множество 2^x, содержащее в точности все возможные подмножества множества x. Формально: $\forall x \exists p \forall y (y \subseteq p \leftrightarrow y \in x)$.

Аксиома 14.5. Схема аксиом выделения. Для любого множества x и любой формулы от одного аргумента $\phi(y)$, такой, что b в нее не входит свободно, найдется такое множество b, в которое входят те и только те элементы из множества x, что $\phi(y)$ истинно. Формально: $\forall x \exists b \forall y (y \in b \leftrightarrow (y \in x \& \phi(y)))$

Определение 14.3. Пересечением множеств x и y называется множество, состоящее в точности из тех элементов, которые присутствуют и в x и в y. Формально: $x \cap y$ — это такое множество z, что $\forall t (t \in z \leftrightarrow t \in x \& t \in y)$

Определение 14.4. Пустое множество $\emptyset$ — множество, которому не принадлежит никакой элемент: $\forall x \neg x \in \emptyset$.

Теорема 14.1.

1. Для любого множества X существует множество $\{X\}$, содержащее в точности X.
2. Если существует хотя бы одно множество, то существует пустое множество.
3. Пустое множество единственно.
4. Для двух множеств существует множество, являющееся их пересечением.

Определение 14.5. Дизъюнктным (разделенным) множеством называется множество, элементы которого не пересекаются. Формально: x дизъюнктно, если $\forall y \forall z (y \in x \& z \in x \& \neg y = z \rightarrow y \cap z = \emptyset)$.

Определение 14.6. Прямым произведением дизъюнктного множества a называется множество $\times a$ всех таких множеств b, что b пересекается с каждым из элементов множества a в точности в одном элементе.

$$\forall b(b \in \times a \leftrightarrow (\forall y(y \in a \rightarrow \exists! x(x \in y \& x \in b))))$$

Аксиома 14.6. Аксиома выбора. Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, непусто. Формально: упражнение.

Аксиома 14.7. Аксиома бесконечности Существует множество N, такое, что:

$$\emptyset \in N \& \forall x(x \in N \rightarrow x \cup \{x\} \in N)$$

Аксиома 14.8. Аксиома фундирования В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x(x = \emptyset \vee \exists y(y \in x \& y \cap x = \emptyset))$$

Аксиома фундирования исключает множества, которые могут принадлежать сами себе (возможно, через цепочку принадлежностей):
$X \in Y \in Z \in X$

Аксиома 14.9. Аксиома подстановки Если задана некоторая функция f, представимая в исчислении предикатов (то есть, есть предикат A, что f(x) = y тогда и только тогда, когда $A(x, y) \& \exists! z A(x, z)$) то для любого множества Y существует множество f(Y) — образ множества Y при отображении f.

Ясно, что данная аксиома перекрывает аксиому выделения. Наличие аксиомы подстановки отличает аксиоматику Цермело-Френкеля от аксиоматики Цермело.

Определение 14.7. Упорядоченная пара Упорядоченной парой двух множеств a и b назовем множество $\{a, \{a, b\}\}$, еще будем записывать его так: $\langle a, b\rangle$

Лемма 14.2. Упорядоченная пара существует для любых множеств, также $\langle a, b\rangle = \langle c, d\rangle$ тогда и только тогда, когда $a = b$ и $c = d$.

Определение 14.8. Бинарное отношение Бинарным отношением на множестве X назовем подмножество множества всех упорядоченных пар элементов из X.

На бинарных отношениях естественным образом вводятся отношения рефлексивности, симметричности и транзитивности.

Определение 14.9. Упорядочивание Отношение R на множестве S упорядочивает X, если это отношение транзитивно и оно образует линейный порядок (строгое неравенство). Отношение вполне упорядочивает S, если к тому же для любого непустого подмножества S выполнено $\exists x(x \in B \& \forall y(y \in B \rightarrow \neg y < x))$.

Также можно ввести понятие максимума, минимума, верхней грани, супремума.

Определение 14.10. Множество x - транзитивное, если $z \in y, y \in x \rightarrow z \in x$.

Определение 14.11. Ординал (порядковое число) — транзитивное, вполне упорядоченное с помощью $\in$ множество.

Рассмотрим ординалы подробнее. Для начала рассмотрим *конечные* ординалы: $0 := \emptyset$; $1 := \{\emptyset\}$; $2 := 1 \cup \{1\}$ и т.п. Существование этих ординалов легко доказать.

Помимо конечных, бывают бесконечные ординалы. Например, таковым является множество N из аксиомы бесконечности. Заметим, что $N \cup \{N\}$ — это новый ординал, не равный исходному.

Определение 14.12. Ординал x называется предельным, если $\neg x = \emptyset \& \neg \exists y (y \cup \{y\} = x)$.

Определение 14.13. Ординал x называется натуральным числом, если любой y, меньший x — это либо 0, либо про него справедливо, что $\exists z (z \cup \{z\} = y)$.

Минимальный предельный ординал мы обозначим ω. Ясно, что любое натуральное число меньше, чем ω.

Операцию $x \cup \{x\}$ можно выбрать за операцию прибавления 1. Для ординалов можно определить арифметические операции $(+)$, $(\cdot)$. Получится некоторое обобщение натуральных чисел со странными свойствами. Скажем, будет справедливо $1 + \omega = \omega$.

Ординалы становятся важными, например, при доказательстве утверждений с помощью трансфинитной индукции: пусть есть некоторое утверждение $P(x)$, определенное на ординалах. Пусть мы можем показать, что из того, что $P(y)$ справедливо на всех ординалах $y < z$, следует, что $P(z)$ тоже справедливо. Тогда $P(x)$ верно для любого ординала. Трансфинитная индукция есть обобщение обычной индукции. Например, с ее помощью доказана непротиворечивость формальной арифметики.

Определение 14.14. Назовем множества X и Y равномощными, если найдется биективное отображение X на Y. Будем записывать это как $|X| = |Y|$. Будем говорить, что множество X имеет мощность не превышающую Y, если найдется инъективное отображение X в Y. Будем записывать это как $|X| \le |Y|$. Будем записывать $|X| < |Y|$, если известно, что $|X| \le |Y|$, но неверно, что $|X| = |Y|$.

Определение 14.15. Кардинальные числа Кардинальное число - такой ординал x, что $y < x \leftrightarrow |y| < |x|$.

Все натуральные числа являются кардинальными. Также, например ω — кардинальное число (еще оно обозначается как $\aleph_0$, если речь идет о мощности множеств). 2^ω — кардинальное число $\aleph_1$, соответствует мощности континуум.

Есть ли какое-нибудь кардинальное число между $\aleph_0$ и $\aleph_1$? Континуум-гипотеза (что никаких других кардинальных чисел между ними нет) была высказана довольно давно, и длительное время была одной из главных проблем в теории множеств. Сначала Геделем было показано, что континуум-гипотеза не противоречит ZF. Утверждение о том, что и отрицание континуум-гипотезы не противоречит ZF, было доказано через 30 лет Коэном.

15 Литература

Возможно, в ходе подготовки вам потребуются дополнительные источники. В таком случае рекомендуется использовать следующие книги:

- Классическое исчисление высказываний и предикатов:

  С. Клини. Математическая логика — М.: Изд-во «Мир», 1973

- Секвенциальное исчисление:

  Г. Такеути, Теория доказательств — М.: Изд-во «Мир», 1978

- Интуиционистская логика:

  Н.К. Верещагин, А. Шень, Лекции по математической логике и теории алгоритмов, Языки и исчисления — МЦНМО, 2002. Также доступно по ссылке `http://www.mccme.ru/free-books/shen/shen-logic-part2.pdf`

- Теорема Геделя о неполноте арифметики:

  Э. Мендельсон. Введение в математическую логику — М.: Изд-во «Наука», 1971.

- Теория множеств:

  А.А. Френкель, И. Бар-Хиллел. Основания теории множеств — М.: Изд-во «Мир», 1966.

  П.Дж. Коэн. Теория множеств и континуум-гипотеза — М.: Изд-во «Мир», 1969.